AMENDMENTS TO THE CLAIMS:

This listing of claims replaces all prior versions of claims in the application.

LISTING OF THE CLAIMS:

Claim 1 (Currently Amended)): In quantum cipher communication using a light signal, a quantum cipher communication system characterized in that:

~~it~~ the quantum cipher communication system uses a phase difference between a weak signal light which is so weak that a change in said weak signal light's quantum mechanical state is detectable and an intense reference light for communicating a privacy key, wherein said phase difference is produced by a sender and a recipient adding a phase on said weak signal light or said intense reference light;

~~it~~ the quantum cipher communication system has ~~a detector~~ two photoconductive diodes which detects said phase difference as a difference signal of said ~~detector~~ photoconductive diodes,

wherein said difference signal is assigned to bit 0 or bit 1 by comparing said difference signal with threshold values which are determined from a quantum-mechanical probability distribution of said difference signal obtained from a plurality of said difference signal assigned bit 1 or bit 0; and

wherein an eavesdropping is detected by said recipient measuring a change in said quantum-mechanical probability distribution of said difference signal, which is produced by the eavesdropping operation.

Claims 2-14 (Canceled).

Claim 15 (Currently Amended): In quantum cipher communication using a light signal, a quantum cipher communication system ~~as set forth in claim 1~~, which comprises a sender's apparatus, a recipient's apparatus and a transmission path connecting between said sender's apparatus and said recipient's apparatus, and is characterized in that

said sender's apparatus comprises:

a light source for a laser beam;

a beam splitting means for splitting said laser beam into ~~said~~ a weak signal light and ~~said~~ an intense reference light;

a phase modulation means for imparting a phase change on ~~making~~ either ~~of~~ said weak signal light or said intense reference light ~~a phase change~~ for every light of said laser beam and

a light attenuation means for attenuating said weak signal light intensity,

said recipient's apparatus comprises:

a phase modulation means for imparting a phase change on ~~making~~ either ~~of~~ said weak signal light or said intense reference light ~~a phase change~~ for said every light transmitted from said sender's apparatus through said transmission path;

a superimposing means for superimposing said weak signal light and said intense reference light, either of which is phase changed by said phase modulation means of said recipient's apparatus;

a pair of photoconductive diodes for converting two output lights from said superimposing means into respective electric signals; and

an amplifying means for amplifying a difference signal between said respective electric signals as said difference signal,

wherein said sender, by using said phase modulation means of said sender's apparatus, imparts to either of said weak signal light or said intense reference light a phase change randomly selected from a set of phase changes predetermined by said sender and said recipient for said every light, and said recipient, by using said phase modulation means of said recipient's apparatus, imparts to either of said weak signal light or said intense reference light a phase change randomly selected from said set of phase changes for said every light, as well as measures said difference signal between said electric signals amplified by said amplifying means;

then, by using a public communication line, said recipient notifies said sender of said phase changes imparted by said recipient;

said sender calculates a total phase difference between said weak signal light and said intense reference light by adding said phase change made and notified by said recipient and said phase change made by said sender, and notifies said recipient of each a light whose total phase

difference satisfy a total phase condition predetermined by said sender and said recipient, as a raw key candidate for being adopted as a privacy key;

then said recipient, for said each light notified as said raw key candidate, assigns bit 1 or bit 0 by comparing said difference signal thereof with ~~said~~ threshold values +X and -X, as assigning bit 1 when said difference signal thereof is equal or greater than said threshold value +X, and assigning bit 0 when said difference signal thereof is equal or less than said threshold value - X, whereby said recipient gets a privacy key;

said sender, for said each light notified as said a raw key candidate, assigns bit 1 or 0 according to a condition regarding said total phase difference, which is predetermined by said sender and said recipient, whereby said sender gets a privacy key;

wherein said threshold values +X and -X are determined from said quantum-mechanical probability distribution;

wherein said eavesdropping is detected by said recipient measuring a change in a quantum-mechanical probability distribution; and

wherein said sender and said recipient can get a privacy key in common with suitable effective detection efficiency and suitable error rate by selecting said threshold values +X and -X.

Claim 16 (Currently Amended): In quantum cipher communication using a light signal, a quantum cipher communication system as set forth in claim 15, characterized in that

said sender's apparatus further comprises:

a movable mirror as said phase modulation means of said sender's apparatus; and

a light attenuator as said light attenuation means,

~~a~~ said transmission path comprising a pair of paths for transmitting said weak signal light and said intense reference light respectively ~~as said transmission path~~,

said recipient's apparatus further comprises:

a movable mirror as said phase modulation means of said recipient's apparatus;

a beam splitter as said superimposing means;

said set of phase changes are 0,90,180, and 270 degrees, and

said total phase condition is either 0 or 180 degrees.

Claim 17 (Currently Amended): In quantum cipher communication using a light signal, a quantum cipher communication system as set forth in claim15, characterized in that

said sender's apparatus further comprises:

~~a~~ said light source for a linearly polarized pulsed light ~~as said light source~~;

a beam splitter for splitting said linearly polarized pulsed light into said weak signal light and said intense reference light as said beam splitting means;

a first long optical path comprising a half wave plate for rotating the polarization of said signal light by 90 degrees, a light attenuator for attenuating said weak signal light intensity as said light attenuating means, a phase modulator making said weak

signal light a phase change for every light of said linearly polarized pulsed light as said phase modulation means of said sender's apparatus, and mirrors; and

a first polarized beam splitter for returning said weak signal light transmitted through said first long optical path and said intense reference light onto a common optical axis, wherein said weak signal light and said intense reference light returned to said common optical axis have a mutual time delay based on the optical path length difference between said first long optical path for said weak signal light and a first short optical path where said intense reference signal reaches to said first polarized beam splitter from said beam splitter, and have mutually orthogonal polarizations,

an optical fiber comprising a single mode optical fiber connected to said first polarized beam splitter, wherein said weak signal light and said intense reference light are transmitted there-through, keeping said mutual time delay and said mutually orthogonal polarizations,

said recipient's apparatus further comprises:

a second polarized beam splitter for splitting said weak signal light and said intense reference light transmitted through said optical fiber;

a second long optical path comprising a half wave plate for rotating the polarization of said intense reference light transmitted through said optical fiber, and mirrors, and a second short optical path comprising a phase modulator for imparting a phase

change on ~~making~~ said weak signal light ~~a phase change~~ for said every light transmitted through said optical fiber as said phase modulation means of said recipient's apparatus, wherein the time delay based on the optical path length difference between said second short optical path and said second long optical path of said recipient's apparatus has the same absolute value and opposite sign to said mutual time delay in said sender's apparatus;

a third polarized beam splitter for superimposing said weak signal light transmitted through said second short optical path and said intense reference light transmitted through said second long optical path as said superimposing means;

~~a~~ said pair of photoconductive diodes for converting two output lights from said third polarized beam splitter into respective electric signals ~~as said pair of photodiodes~~; and

an amplifier for amplifying a difference signal between said respective electric signals as said amplifying means,

said set of phase changes are 0,90,180, and 270 degrees, and

said total phase condition is either 0 or 180 degrees.

Claim 18 (Previously Presented): A quantum cipher communication system as set forth in claim 17, characterized in that a third light polarizer is provided in an output side of said single

mode optical fiber for making a correction for a disturbance of polarization of said intense reference light.

Claim 19 (Currently Amended): A quantum cipher communication system as set forth in any one of claims 15 to 17, characterized in that in addition to said phase modulation of both said sender's and recipient's apparatuses used to transmit said privacy key, a phase modulation is imparted having a value later determined to make a correction for a fluctuation of the difference in optical path between said transmission path of said intense reference light and said transmission path of said weak signal light which develops by reason of an external cause.

Claim 20 (Currently Amended): A quantum cipher communication system as set forth in claim 19, characterized in that said phase modulation of both said sender's and recipient's apparatuses used to transmit said privacy key and said phase modulation to make a correction for said fluctuation are randomly repeated.

Claim 21 (Previously Presented): A quantum cipher communication system as set forth in any one of claims 15 to 17, characterized in that eavesdropping is detected on the basis of an increase in an error rate of said difference signal.

Claim 22 (Previously Presented): A quantum cipher communication system as set forth in any one of claims 15 to 17, characterized in that eavesdropping is detected on the basis of a change in a Wigner distribution function that indicates a quantum mechanical state of said weak signal light.

Claim 23 (Previously Presented): A quantum cipher communication system as set forth in any one of claims 15 to 17, characterized in that for said pair of photoconductive diodes, use is made of silicon photoconductor diodes when said light source has a wave length of 600 nm to 900 nm, and of InGaAs photoconductor diodes when said light source has a wave length of 1000 nm to 1500 nm.

Claim 24 (Previously Presented): A quantum cipher communication system as set forth in any one of claims 15 to 17, characterized in that said weak signal light has a typical intensity corresponding to as small as single photon, and said intense reference light has a typical intensity corresponding to photons as large as 10 millions in number.